PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G08B 25/01 — A1

(11) International Publication Number: **WO 98/04967**

(43) International Publication Date: 5 February 1998 (05.02.98)

(21) International Application Number: PCT/GB97/00241

(22) International Filing Date: 28 January 1997 (28.01.97)

(30) Priority Data:
9615597.3 25 July 1996 (25.07.96) GB

(71)(72) Applicants and Inventors: COLLINS, Peter, David [GB/GB]; 2 Spencers, Hawkwell, Hockley, Essex SS5 4LW (GB). ROYER, Karl, William [GB/GB]; 14 Buttermere Gardens, Aylesham, Kent CT3 3LT (GB). BOWYER, Mark, David, James [GB/GB]; 7 Southleigh Road, Havant, Hants PO9 2RR (GB).

(74) Agent: LEEMING, John, Gerard; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5LX (GB).

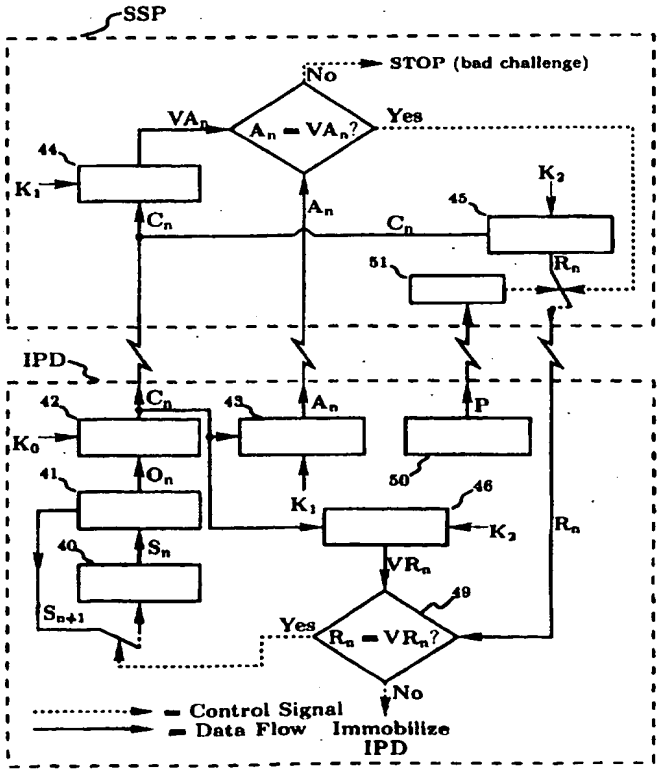
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: IMMOBILISATION PROTECTION SYSTEM FOR ELECTRONIC COMPONENTS

(57) Abstract

An electronic security system that embeds electronic immobilisation protection devices (IPDs) in electronic products and components. IPDs have controlled access to a security service provider (SSP). At power on, and periodically thereafter, the IPD sends a cryptographically secure "challenge" to the SSP. If a part has not been reported stolen, then the SSP replies with a valid cryptographically secure "response", otherwise it replies with an invalid "response". If the IPD receives an invalid "response", or when a limited time has elapsed without a "response", it renders the part inoperative. A valid "response", inside the time limit, allows the part to function normally. A stolen and recovered product can be identified and traced to its rightful owner, who contacts the SSP to re-enable the product. IPDs allow specific parts to function normally for a limited period of time, so that existing hardware, software and network resources can be utilised to communicate to the SSP.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Immobilisation Protection System for Electronic Components

This invention relates to security for electronic products and systems.

The theft of electronic products (e.g. computer, video and hi-fi appliances) and VLSI components (CPUs and SIMMs) has become a matter of great concern to both companies and individuals. Currently, most products and components lack unforgeable serialisation capable of linking them to their registered owner. As a result, criminals have the incentive that stolen equipment can be re-sold as new with negligible depreciation.

Currently, such crime is deterred by physical security systems protecting premises and/or individual equipment. Many of these systems hinder the normal use of such equipment and pose no real deterrent to the determined criminal.

The knowledge that the ownerships of products or components are quickly traceable is a significant deterrent to the criminal. However, even if the equipment is traceable, the criminal can re-sell equipment which is still fully functional. A greater level of deterrent to the criminal is the publicised knowledge that, taken away from an authorised user, a product or component is rendered inoperative.

US-A-4,759,062 discloses a means for immobilising micro-processor controlled electronic equipment using a "challenge-response" authentication scheme between equipment and an authorised service centre. The equipment sends a challenge that is communicated to the authorised service centre which computes a response which is communicated back to the equipment. If the equipment receives an incorrect response then it renders the equipment inoperative. The cryptographic algorithm used to compute responses in each piece of equipment is identical, in such a way that, if the algorithm in one piece of equipment is compromised, then all other equipments are compromised.

GB-A-2,251,503 discloses a security system that prevents unauthorised parts embedded with electronic protection equipment from being used in a car. The protection equipment is added to a part in such a way that removal of the protection equipment would cause terminal damage to the protection equipment. This system employs a "challenge-response" authentication scheme between a controller and its parts (i.e. in the opposite direction to the above art). The controller sends a coded signal to the part which processes the signal and provides a response. If a part answers the challenge incorrectly then the controller sends immobilisation commands to that part and other parts in the system, in order to render

them inoperative.

However, components removed from a protected vehicle and moved to an unprotected vehicle will function normally and furthermore lack means of unforgeable identification.

Therefore according to the present invention there is provided an electronic immobilisation device (IPD), for protecting electronic equipment associated therewith, and for use with a remote validating means (SSP), the immobilisation device comprising:

means for generating a challenge code (C_n);

means for providing an identification code (P) uniquely identifying the electronic immobilisation device;

output means for outputting said challenge code and said identification code to said validating means (SSP);

input means for receiving a response code (R_n) from said validating means (SSP);

checking means for comparing said response code (R_n) with said challenge code and providing a control signal indicating whether said comparison is valid; and

inhibiting means for inhibiting or restricting operation of the protected electronic equipment if said control signal is not valid.

Throughout the specification the term equipment refers either to a product, module or component.

Protected electronic equipment is provided with an embedded electronic immobilization protection device (IPD), such that from power on, the IPD can control the useful operation of the equipment.

The IPDs may be embedded within the equipment at one of three levels as:

(i) an additional component inside a housing or mounted on a printed circuit board;

(ii) an additional component bonded to components, particularly important, essential or high value components; or

(iii) additional logic integrated at mask (or multi-chip module) level into essential or high value integrated circuits.

Essential components are those without which the product of which they form a part cannot function usefully. Level (i) provides the lowest level of deterrent because it may be possible to by-pass the IPDs. Furthermore, there is no deterrent against extraction of high values components. In level (ii) the IPD is bonded to and encapsulates components in such a way that by-pass or removal of the IPD causes terminal damage to the protected component. Level (iii) provides the highest level of deterrent because the IPD is truly integral with the protected component, making by-pass extremely difficult.

The rightful owner of a piece of protected equipment is provided with controlled access to a security service provider (SSP). IPDs are programmed by the manufacturer or retailer with a unique part number (P), one or more cryptographic functions, and cryptographic keys. To initiate protection, the rightful owner registers the IPDs with a SSP. The manufacturer or retailer advises the SSP of the necessary cryptographic functions and keys, using a secure channel.

When protected equipment is powered on, a communication link between the IPDs and the SSP is established. This link can involve dedicated functions and communication paths within the product. Alternatively, the pre-existing microprocessor and communication units within the product can be programmed to provide the link. Once the link is established, each IPD sends its part number P together with a random "challenge". The SSP uses the received part number P to retrieve the appropriate cryptographic function(s) and cryptographic key(s) from a database. The SSP can then use the challenge, together with the retrieved function(s) and key(s) to compute a cryptographically secure response.

If the product or component containing an IPD has not been reported stolen, then the SSP replies with a valid cryptographically secure "response", otherwise it replies

with an invalid "response". An invalid "response" could be no response at all. If the IPD receives an invalid "response", or when a time limit has elapsed without a valid "response", then it renders the protected equipment inoperative. If the IPD receives a valid "response", inside the time limit, then it allows the protected equipment to function normally. In either case, if the time limit, measured from power on or some other appropriate point, has elapsed and the IPD has not received a valid "response", then it disables the protected equipment. The time limit is short enough (typically a few minutes) to prevent any useful operation of the protected equipment, but sufficient to allow time to send and receive the required sequence of challenges and responses from the SSP.

The IPD can be used in combination with the SSP to provide authorised users with a means to uniquely and unforgeably identify protected equipment. The IPD and SSP can provide this capability in a number of ways.

One such way, that uses a uni-directional protocol, is to provide access to a cryptographically secure checksum derived from the combination of the part number P, cryptographic key information and a randomly generated code from the IPD. By validating two or more consecutive checksums, the SSP can be sure the IPD part number

corresponds to the key information held in the SSP database.

A second way, that uses a bi-directional protocol, carries out a normal validation process whereby the SSP responds correctly to a challenge issued by recovered equipment and the user monitors the status of the equipment. If the equipment is operational then its part number is genuine. If the equipment is immobilised then the user can infer that the IPD has been tampered with.

Methods of identification, such as those described above, provide unique identification in that the code sequence used to perform the identification is unique to each IPD and, furthermore, is unforgeable in that replaying previous code exchanges between the IPD and SSP will not allow positive identification of the protected equipment. In the latter realisation, a unique response from all IPDs to a given challenge is required. This can be achieved by using a unique cryptographic key for each device or by using the unique part number P in the computation and verification of the cryptographically secure response.

By using this unique and unforgeable identification, a stolen and recovered product containing one or more IPDs can be positively identified and traced to its registered owner. When returned, the registered owner contacts the

SSP in order to authorise the SSP to supply valid responses to the protected equipments, after which, the protected equipments function as normal.

Some portable equipment maintain continuous power to specific components. To ensure such equipment is immobilized in the wrong hands, the IPD may be arranged so that the "challenge - response" cycle is repeated periodically, e.g. every eight hours. The duration of this interval can be varied to suit organizational or operational requirements.

Some prior art systems are vulnerable to disclosure of their principle of operation. A criminal could either monitor an authorised user's challenges and responses or submit their own challenges to an SSP and monitor the response. By doing this a series of challenge-response data can be accumulated and the coding system used in the SSP/IPD deciphered. Once this is done the criminal can calculate a valid response to any challenge, for example by correctly duplicating the function of the SSP.

For extra security, use of a unique cryptographic key in each IPD protects the concept of the system from compromise, i.e. if the keys within a single IPD are compromised the system as a whole is not compromised. Thus even if the operation of the system is known, it is

still necessary to find out the unique key for each IPD to use the protected equipment. The security of the system may be further enhanced by allowing the manufacturers and system operators to agree their own algorithms. However, it is in the interests of the manufactures and operators to choose "strong" cryptographic algorithms. The term "strong" refers to algorithms that remain secure in the event of exposure, i.e. if the algorithm within one IPD is exposed then IPDs using the same algorithm are not compromised. Prefixing the part number P to the "challenge" identifies the IPD to the SSP and allows the SSP to select the correct algorithms and keys for the IPD requesting the "response." Furthermore, the SSP uses the part number P to search in a database containing the status of IPDs, e.g. unregistered, registered, stolen, or recovered, to confirm the status of the IPD.

An SSP can provide its users with several modes of connection: (i) circuit or packet access to a central security server; (ii) packet access to a local security server; or (iii) direct access to a plug-in security server.

Mode (i) is a centralized mode whereby the product connects to a central security server using any available means of communication, e.g. an individual can use a modem to connect via a PSTN; a company can use its LAN to

connect via a WAN gateway.

Mode (ii) is a distributed mode of operation in which local servers connect when necessary to a central security server. Local security servers contain at least one IPD per server, so that, in the event a server is stolen, equipment stolen from the same premises is not compromised. There are two types of local security server: (i) a slave server that computes "responses"; (ii) a cache server that requests several "challenges" in advance and stores the "responses" obtained from a central server. If possible, the local server uses volatile storage. However, information in non-volatile storage is stored, encrypted and decrypted on-the-fly. A single local server might be contained in a house or small business, whereas several might be used in large company or organization. Consumer electronics inside a house can communicate to a local server using an infra-red network. Large office buildings might use a hierarchy of cache servers connected to a slave server.

In mode (iii), a product has direct connection to a smart-card (or similar device) that computes "responses". The smartcard contains the key information necessary to acknowledge the IPDs within the product it serves. When the product is unused, it is the users responsibility to remove and store the smartcard safely, in order to prevent

the product from operating. The smartcard itself has a given lifetime that once exceeded renders the card useless. The smartcard can be reactivated by the SSP. If a product or component is stolen then the smartcard can be presented to an insurer as proof of immobilization.

Users may wish to purchase products and components with the IPD security not activated. At some later date, the user can enable the IPD security and enter the system by contacting an SSP. This allows equipment fitted with IPDs to be used as normal in systems without connection to and authorisation of an SSP. This also avoids the need to manufacture two types of device, i.e. with IPD and without IPD.

Once enabled, the IPD security can preferably not be disabled. However, SSP users could leave the system by obtaining a lifetime smartcard covering the users products and components. However, once the user obtains such a card, the SSP can offer the user no security for these products and components.

The embedded and cryptographically secure natures of IPDs is sufficient so that individuals, outside the realms of approved manufacturers and the SSPs, including the rightful owner, are unable to provide a method, or gain information, to by-pass or enable IPDs without a valid

"response" from an SSP.

IPDs incorporated into data storage products can provide data security in addition to immobilization. For example, the control processor on a fixed disk can be programmed, from power on, not to transfer data on some or all of the disk until a valid "response" is obtained from an SSP. If the disk is reported stolen, then data on the disk in the specified partitions cannot be read at all, not even for a limited time.

IPDs may be used to provide controlled access to the equipments they immobilize. For example, outside working hours, the SSP can provide invalid responses to selected IPD "challenges", in order to ensure that certain items of equipment cannot be used outside pre-determined hours.

The SSP can store a day-to-day record of the products and equipment that send IPD "challenges". The SSP can use this record to provide an audit facility to its customers. This is especially useful for computer memory modules, plug-in cards and peripherals that are moved around in a large organization, e.g. the SSP can provide day-to-day lists of products containing IPDs that have been moved from one machine to another.

The length of time between "challenge - response" cycles

can be lowered in order to provide customers with a usage monitoring capability. However, the SSP cannot obtain such information when equipment is switched on and is unused.

Furthermore, the use of IPD's can be extended for use in all manner of verification purposes. For example, credit cards or ID cards could be provided with IPD's using smart card technology, such that they do not provide data or authorisation if they are lost or stolen etc.

By operating an alternate challenge response mechanism, IPDs can be used to grant access to restricted hardware and software services. The party providing the service(s) advises the SSP of what service(s) the said IPD can be granted access to. When a service user requests a service from a given party, the party operating the service sends two challenges: the first to a nominated IPD, within the equipment of the service user, and the second, a copy of the first, prefixed with an identifier for the requested service, to the SSP. Both the SSP and the IPD provide the party with responses to the challenge. If the user has been granted access to the requested service (determined by the received identification code), then the SSP answers the party's challenge correctly, otherwise, it answers incorrectly. Finally, the party compares the responses received from the SSP and IPD. If they are identical,

then the party grants access to the requested service, otherwise, it denies access. In this scheme, the party providing the service has no knowledge (or need to know) of the cryptographic algorithms and keys held within the IPDs and the SSP.

The present invention will be more clearly understood from the following description, given by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a flow diagram that shows the computational functions inside an embodiment of an IPD and SSP;

Figure 2 is a personal computer system incorporating IPDs;

Figures 3 and 4 show two methods in which a single PC can connect to an SSP; and

Figures 5, 6 and 7 show how corporate users with existing networks can connect to an SSP.

Referring to figure 1. The IPD "challenge" is a non-recurring cryptographically secure random number. To achieve the non-recurring property, the IPD contains a non-volatile state register 40. The IPD loads the contents of the state register S_n, into a sequence generator 41 from which a new unique state, S_{n+1} is

generated, but not immediately used. The output of the sequence generator, O_n, is fed into a cryptographic encoder 42. The output, O_n is derived from S_n and preferably not reversibly such that S_n is not derivable from O_n. This can be achieved, for example, by only using some of the bits of S_n to produce O_n. The encoder 42 uses a cryptographic function or algorithm to code the input O_n using a key K_0 stored inside the IPD. The output C_n, from the encoder 42 is the "challenge". The key K_0 need not be unique amongst all IPDs. However, if the key K_0 is unique, then each IPD produces a unique sequence of cryptographically secure random "challenges". This level of refinement makes the system more difficult to attack.

To allow an SSP to filter "challenges" from rogue users, the IPD incorporates a means for the SSP to validate "challenges". To achieve this the IPD must uniquely identify itself to the SSP. For example, an attacker, wishing to deny SSP service from legitimate users could flood SSP connections with rogue "challenges" and possibly monitor the responses. One such means to prevent this is to send an authenticator, A_n, derived from the "challenge", C_n, using a second encoder 43 with the key, K_1, stored in the ROM.

At the SSP, the received "challenge" is fed into an encoder 44 with the key K_1, obtained from a lookup database

based on the part number *P* of the IPD. The first encoder 43 and second encoder 44 carry out the same coding operation as each other. If the output, VA_n, of encoder 44 and the received authenticator A_n from the IPD are the same then the "challenge", C_n, is valid. The received "challenge" C_n is fed into a third encoder 45 utilising the key K_2, obtained from the lookup database using *P* generated by the part number generator 50. The output from the third encoder is the cryptographically secure "response", R_n. Returning to the IPD, C_n is fed into a fourth encoder 46 utilising the key K_2, stored inside the IPD. The third 45 and fourth 46 encoders carry out the same coding operation. The output, VR_n, of the fourth encoder 46 and the received "response" R_n (from the SSP) are compared by a comparator 49 and if they are equal, then the protected product or component is allowed to function and the register 40 is loaded with the state S_{n+1}. If the comparison 49 fails, then the product or component is disabled and the register 40 remains in its original state, S_n. This means that an unauthorised user is unable to monitor the sequence of challenges from the IPD as these only change when a valid challenge-response cycle occurs.

The SSP monitors 51 the part number P and checks to ensure that the corresponding IPD has not been reported stolen or otherwise. If so, an invalid response or no response is

output.

The cryptographic function used in the encoders 42-46 shown in figure 1 can be block cipher algorithms in which the key is directly applied. Alternatively, the cryptographic function can be a secure hash function in which the key is mixed with the input to the function. The non-recurring property of the "challenge" is highly desirable, but not essential. An alternative is to use a true random number generator in place of the non-volatile state register and sequence generator.

A personal computer (PC) system incorporating IPDs 71 72 is shown in figure 2. Internal IPDs are connected via a simple bus 62 to the IPD interface adaptor 65, integrated on the PC motherboard 70. Alternatively, the IPD interface adaptor is a plug-in card. External IPDs 72 are connected to external IPD bus 67 and use a buffered connection 66 to the IPD interface adaptor 65. Alternatively, external IPDs can use existing connections to the computer, eg. printers can use a parallel or serial port and SCSI peripherals can use the SCSI bus. The PC has at least one means to access the SSP, eg. a network adaptor 73, a smartcard interface (see figure 3), or a modem attached to a PSTN (see figure 4).

When the PC is turned on, IPDs in system critical

components 60 61 are enabled, for a limited period of time, allowing the computer to function normally. This time is sufficient for the PC to load its operating system, establish communication with the SSP, to send "challenges" and receive "responses". The details of procedure are as follows. The PC loads its operating system and starts a special process that (i) collects part numbers and "challenges" from the components 60 61 63 68 using the IPD interface adapter 65; (ii) establishes a connection to the SSP; (iii) sends the part numbers and "challenges" to the SSP; (iv) receives "responses" from the SSP; and (v) dispatches "responses" to the appropriate IPDs. Any component in the PC system that does not belong to its rightful owner receives an invalid "response" from the SSP. In this case, the IPD will disable the component after an additional short delay (to allow the computer fail safe). If all "responses" are valid, then the computer continues to function normally and with system-critical functions enabled. A key feature is, therefore, that existing hardware (such as 60 61) and software (and network 69 73) resources within the PC system are used to communicate with the SSP. The path between the IPD interface, on the PC motherboard, and the SSP can be encrypted in order to prevent an eavesdropper auditing the property of an individual or organization.

Figure 3 shows a PC 30 connected to a smartcard interface

31. The user is issued a smartcard 32 by the SSP 34. On receipt of the smartcard, the user is able to operate his system for a set period (e.g. one year), after which the SSP can use manual or electronic means to update the card, e.g. using a modem (not shown) to establish a communication link from the smartcard to the SSP, or by returning the card to the SSP for replacement or re-validating.

Figure 4 shows a PC 20 that connects to an SSP 23 using a modem 21 connected to a public switched telephone network (PSTN) 22. The connection can be to a modem server located in the SSP. Alternatively, the PC can dial-up a local Internet provider and communicate to an Internet connected SSP.

Figure 5 shows a PC 10 that connects to an SSP 14 via a LAN 11, a WAN 13, and a firewall 12. Figure 6 shows a PC 1 that connects to local security server 6 via a LAN 2. In turn, the local security server connects to the SSP 5 via (i) a firewall 3 and WAN 2 and/or (ii) a modem link (not shown). The local security server reduces the WAN bandwidth required by a large organization.

Figure 7 shows a system that uses a hierarchy of security servers inside a large customer premises 90. The PCs 102 103, on separate LAN subnets 91, 96, connect to local

cache security servers 92 94. The LAN subnets 91 and 96 are connected to a backbone LAN 97 by the router/firewalls 93 and 95. The LAN 97 has connected a slave security server 98 that has access via a gateway/firewall 99 to a WAN 100. In normal operation, the cache servers 92 94 communicate "challenge - response" packets directly to the slave security server 98. In the event that the slave server fails, or is unable to identify a part number, the cache servers can communicate "challenge - response" packets off site with the SSP 101.

CLAIMS

1. An electronic immobilisation device (IPD), for protecting electronic equipment associated therewith, and for use with a remote validating means (SSP), the immobilisation device comprising:

means (40,41,42) for generating a challenge code (C_n);

means (50) for providing an identification code (P) uniquely identifying the electronic immobilisation device;

output means for outputting said challenge code and said identification code to said validating means (SSP);

input means for receiving a response code (R_n) from said validating means (SSP);

checking means (49) for comparing said response code (R_n) with said challenge code and providing a control signal indicating whether said comparison is valid; and

inhibiting means for inhibiting or restricting operation of the protected electronic equipment if said control signal is not valid.

2. A device according to claim 1 further comprising a first processing means (43) to produce an authentication code (A_n) from said challenge code, wherein

said output means outputs said authentication code (A_n) to said validating means (SSP).

3. A device according to claim 2, wherein the first

processing means utilises a cryptographic algorithm using a first key (K_2).

4. A device according to claim 2 or 3, further comprising second processing means (46) for processing said challenge code using a method uniquely corresponding to the identification code to produce a check code (VR_n), wherein

said checking means (49) compares said check code (VR_n) with said response code (R_n) to provide said control signal.

5. A device according to claim 4, wherein the second processing means utilises a cryptographic algorithm using a second key (K_1).

6. A device according to any one of claims 1 to 5, wherein the generating means (40, 41, 42) comprises a sequence generator (40, 41) for generating a seed code (O_n) and third processing means (42) for coding the seed code (O_n) to provide said challenge code (C_n).

7. A device according to claim 6 wherein, the third processing means utilises a cryptographic algorithm using a key (K_o).

8. A device according to claim 6 or 7, wherein the seed

code (O_n) is derived from a sequence code (S_n) produced by the sequence generator (40, 41) and wherein the sequence code is changed each time said checking means (49) provides a valid control signal.

9. A device according to claim 8 wherein the seed code (O_n) is irreversibly derived from a sequence code (S_n).

10. A device according to claim 3 and claim 5, wherein the first and second processing means use different algorithms.

11. A device according to claim 3 and claim 5 or claim 10, wherein the first key (K_2) and the second key (K_1) are different.

12. A device according to any of the preceding claims wherein the electronic immobilisation device (IPD) is associated with the protected electronic equipment by being: electrically connected to, attached to, enclosed in or integrated with the protected electronic equipment.

13. A device according to any one of the preceding claims wherein the inhibiting means allows at least partial operation of the protected electronic equipment for a pre-determined time without having received a valid control

signal.

14. A security system incorporating an electronic immobilisation device (IPD) according to any one of the preceding claims and a validating means (SSP);

the validating means (SSP) comprising:

fourth processing means (45) for coding the challenge code received from the electronic immobilisation device, to produce the response code (R_n), and

means (52) for selectively outputting the response code (R_n).

15. A system according to claim 14, when dependent on claim 2, the validating means (SSP) further comprising:

fifth processing means (44) for coding the first challenge code (C_n) to produce an authentication validation code (VA_n);

comparing means for comparing the authentication code (A_n) from the electronic security device with said authentication validation code (VA_n), wherein said selective output means (52) does not output the response code if the comparison of the authentication code (A_n) and the authentication validation code (VA_n) is not valid.

16. A system according to claims 14 or 15, wherein the validation means further comprises identification code (P) validation means (51) wherein said means for selectively

outputting the response code (R_n) is inhibited if said part number (P) is invalid.

17. A method of validating an immobilisation device (IPD) for protecting electronic equipment comprising in the protection device (IPD):

generating (40, 41, 42) a challenge code (C_n);

outputting to a validating means (SSP) the challenge code (C_n) and an identification code (P) uniquely identifying the immobilisation device (IPD);

receiving a response code (R_n) from said validating means;

comparing said challenge and response codes; and where said comparison is valid, enabling said protected electronic equipment.

18. A method according to claim 17, further comprising the steps of:

coding (43) the challenge code (C_n) to produce an authentication code (A_n) and, outputting the authentication code to the validating means (SSP).

19. A method of validating an immobilisation device (IPD) for protecting electronic equipment comprising the steps of:

receiving a challenge code (C_n) from said immobilisation device (IPD);

coding the challenge code (C_n) to produce a response code (R_n);

selectively outputting the response code (R_n).

20. A method according to claim 19 further comprising the steps of:

coding the challenge code (C_n) to produce an authentication validation code (VA_n);

receiving an authentication code (A_n) from said immobilisation device;

comparing said authentication code (A_n) and said authentication validation code (VA_n);

inhibiting output of said response code (R_n) if the comparison of said authentication code (A_n) and said authentication validation code (VA_n) is not valid.

21. An electronic immobilisation device (IPD), for protecting a electronic equipment associated therewith, and for use with a remote validating means (SSP), the immobilisation device comprising:

means (40,41,42) for generating a challenge signal (C_n);

output means for outputting said challenge signal to said validating means (SSP);

input means for receiving a response signal (R_n) from said validating means (SSP); and

checking means (49) for comparing said response

signal (R_n) with said challenge signal and providing a control signal;

means for inhibiting or restricting operation of the protected electronic equipment if said control signal is not valid.

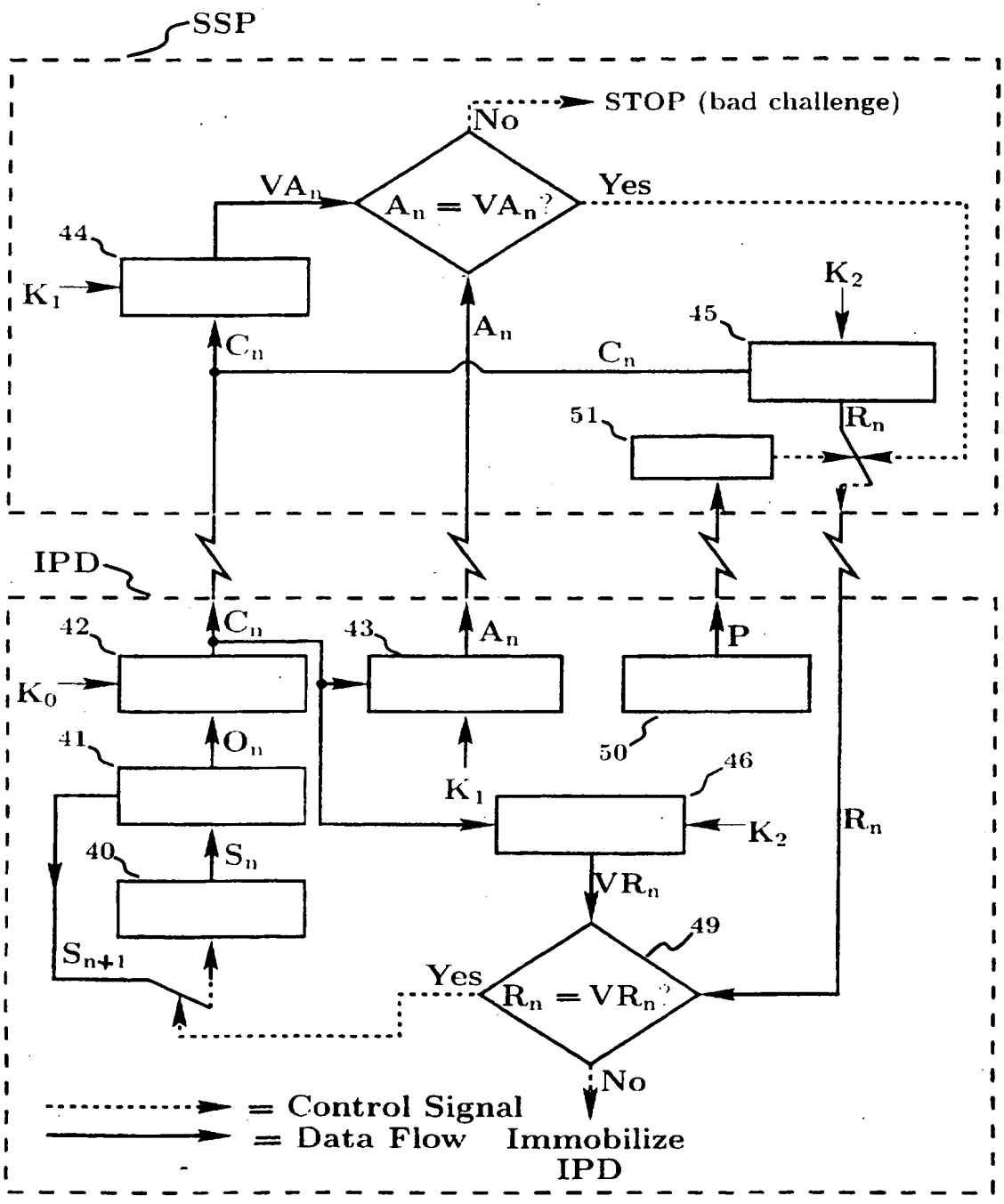


Figure 1

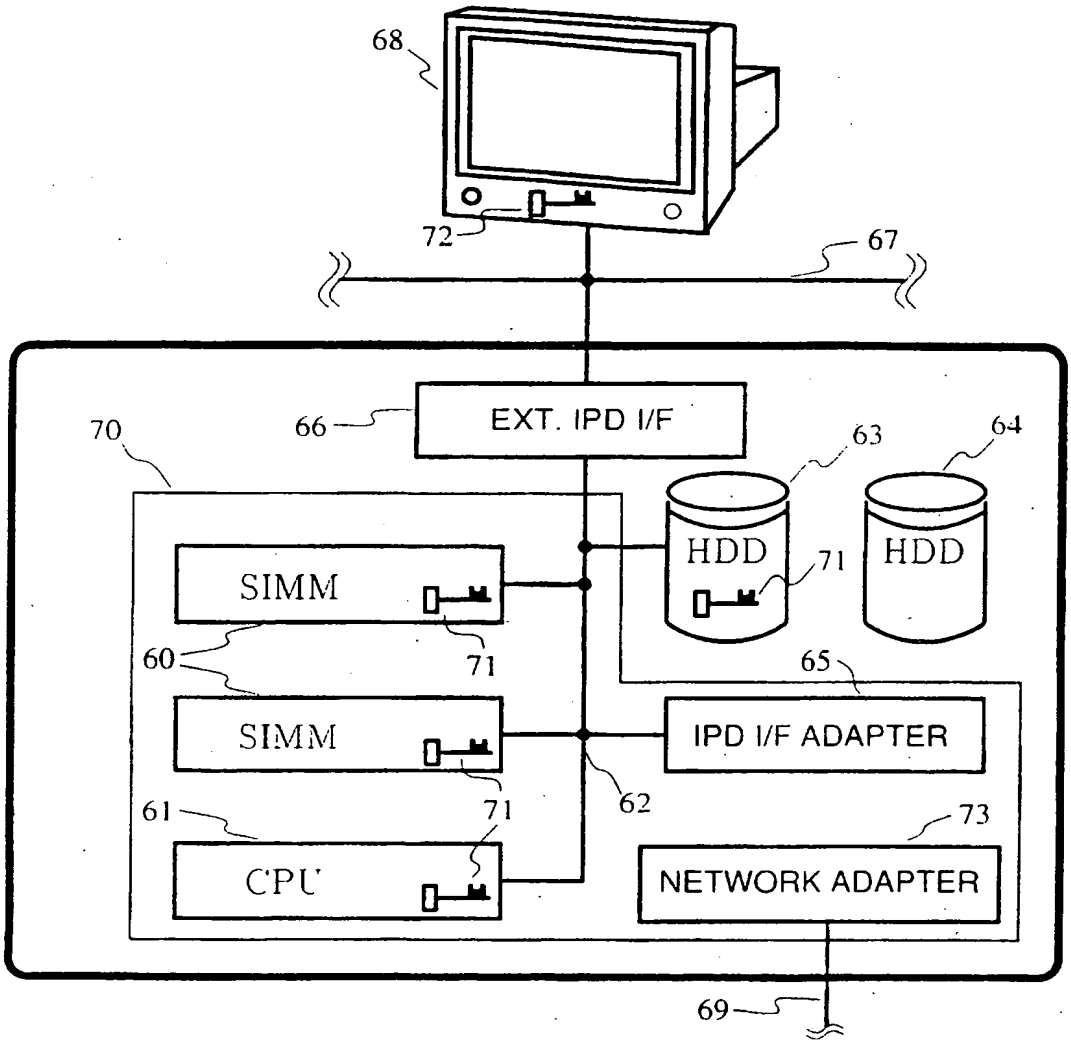


Figure 2

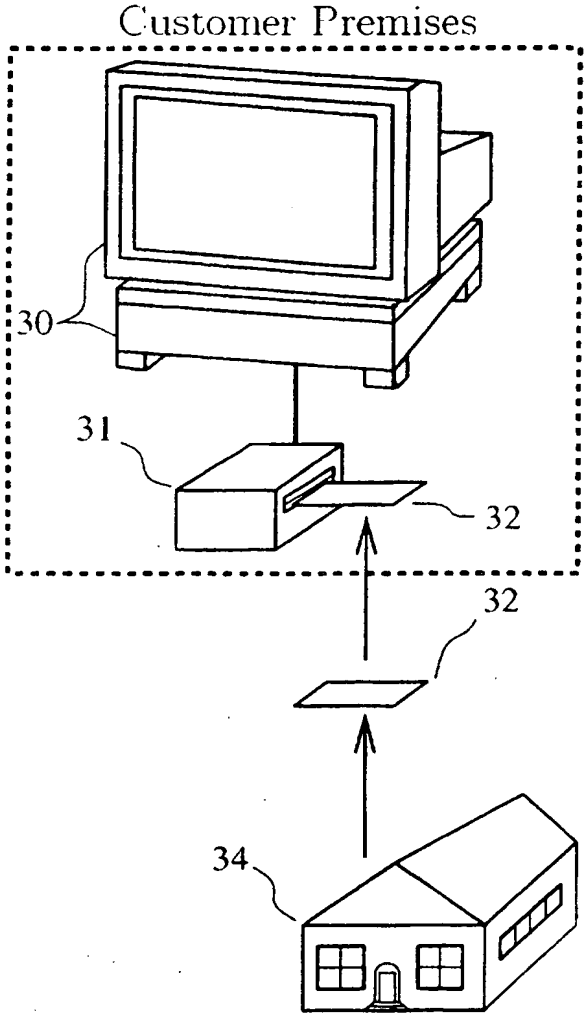


Figure 3

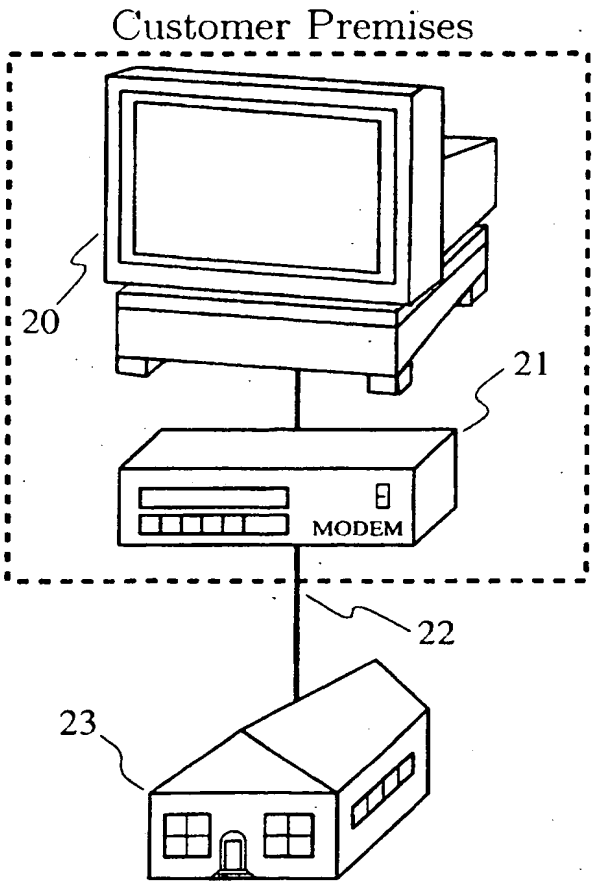


Figure 4

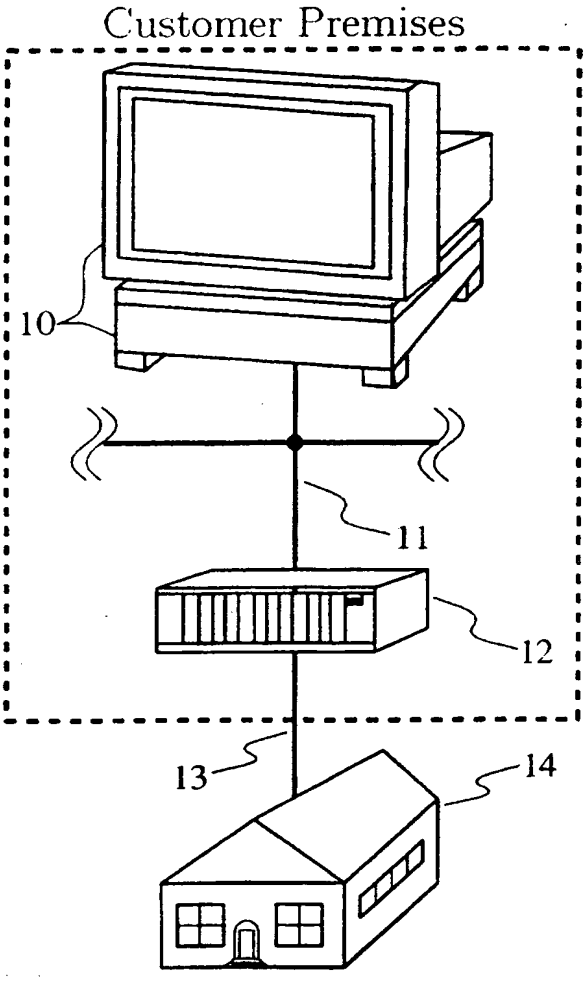


Figure 5

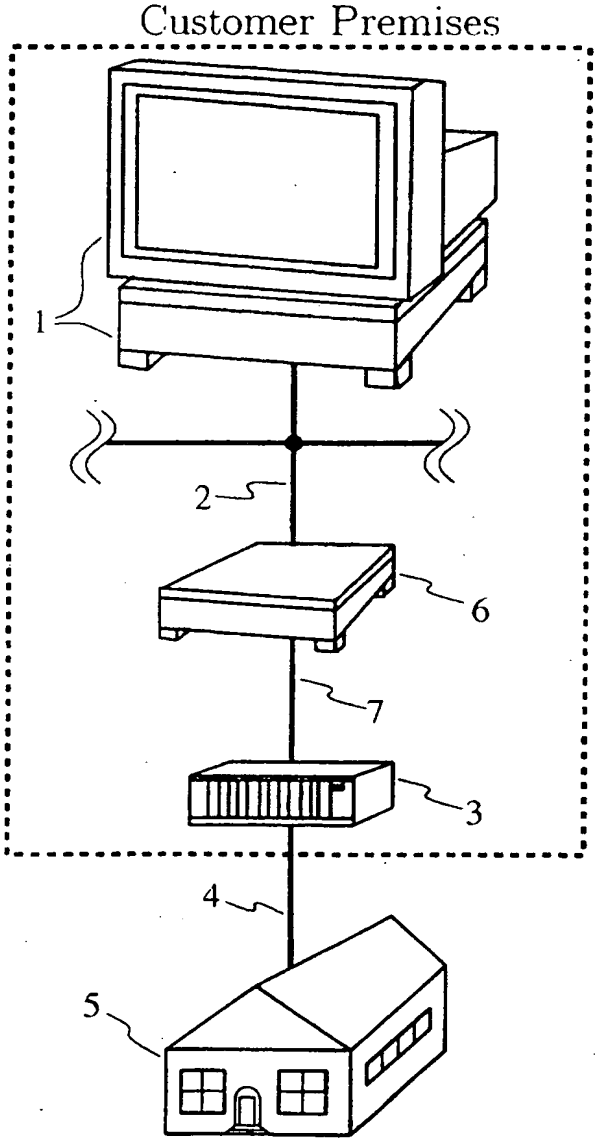


Figure 6

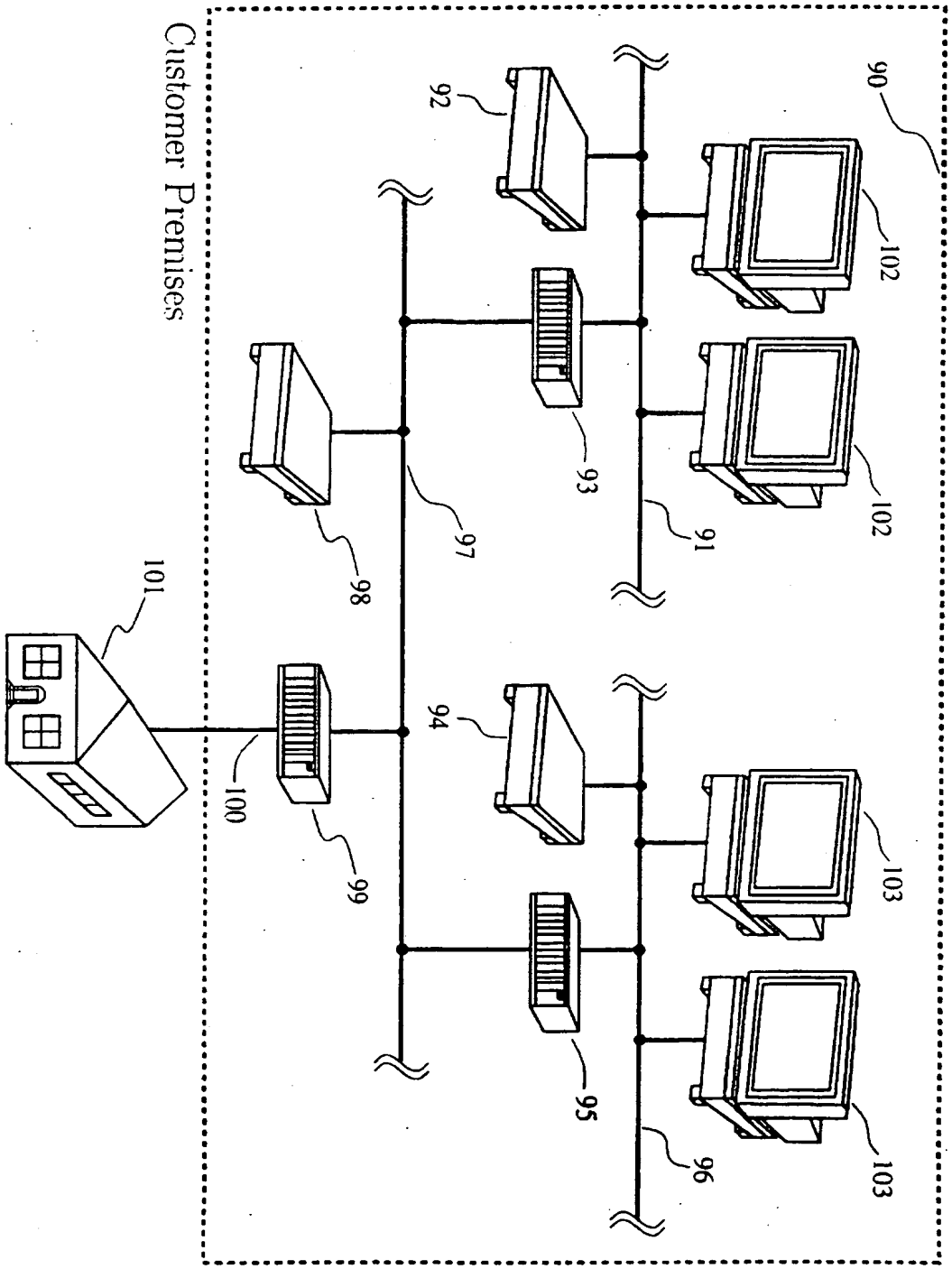


Figure 7

INTERNATIONAL SEARCH REPORT

onal Application No
PCT/GB 97/00241

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G08B25/01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96 03728 A (KANG BALJIT SINGH) 8 February 1996 see the whole document	1,17,19, 21
Y	EP 0 588 519 A (AMERICAN TELEPHONE & TELEGRAPH) 23 March 1994 see column 3, line 11-40; figures 1-5	1,17,19, 21
A	EP 0 387 581 A (BLAUPUNKT WERKE GMBH) 19 September 1990 see the whole document	1-21
P,X	EP 0 740 037 A (HEWLETT PACKARD CO) 30 October 1996 see the whole document	1,17,19, 21

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 1997	22.05.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 97/00241

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9603728 A	08-02-96	AU 2986495 A	22-02-96
		GB 2304443 A	19-03-97
EP 0588519 A	23-03-94	US 5311596 A	10-05-94
		CA 2104849 A	01-03-94
		JP 6204998 A	22-07-94
EP 0387581 A	19-09-90	DE 3908029 A	13-09-90
		DE 3918052 C	22-11-90
		DE 59005401 D	26-05-94
		ES 2054121 T	01-08-94
EP 0740037 A	30-10-96	JP 8305461 A	22-11-96